SYHUNT CODE: GUIA DE INTRODUÇÃO

As informações contidas neste documento se aplicam a **versão 6.9.14** do Syhunt Code.

COMO REALIZAR UM SCAN DE CÓDIGO

A análise de código-fonte do Syhunt pode revelar múltiplos tipos de vulnerabilidades em aplicações web e móveis, e também identificar áreas chave do código que precisam de revisão. A funcionalidade de análise estática de código-fonte detecta cross-site scripting, inclusão de arquivos, injeção de SQL, execução de comandos e problemas de validação. Inicialmente somente PHP era suportado. Atualmente, múltiplas linguagens de programação web e mobile são suportadas.

LINGUAGENS SUPORTADAS (WEB)

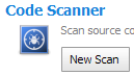
- </> ASP Clássico (VBScript e JavaScript)
- </> ASP.Net (C# e VB.Net)
- </> Java (JEE / JSP)
- </> JavaScript (Client and Server-Side, Node.js, Angular, AngularJS, Express.js e Koa.js)
- </> Lua (ngx_lua, mod_lua, CGILua e Lua Pages)
- </> Perl
- </> PHP
- </> Python (CGI, Django, mod_python e WSGI)
- </> Ruby (Rails e ERB)
- </> TypeScript (Angular)

LINGUAGENS SUPORTADAS (MOBILE)

</> Java (Android)
</> Swift (iOS)
</> Objective-C, C & C++ (iOS)
</> JavaScript (incluindo Node.js, Angular, AngularJS, Express.js & Koa.js)

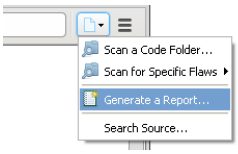
Siga este guia para aprender como realizar um scan de código-fonte e gerar um relatório de vulnerabilidades.

1. Abra Syhunt Hybrid e clique no ícone do Syhunt Code ou no botão New Scan (Novo Scan) na página inicial.



2. Selecione um diretório de código-fonte, arquivo de código-fonte ou um arquivo APK.
3. Selecione um método de scan. Recomendamos o Application Code Scan (Default), método padrão que procura por todas as vulnerabilidades usando as configurações recomendadas - os diferentes métodos são explicados no documento Métodos de Varredura.
4. Pressione o botão **OK** para iniciar o scan.

No final da varredura, você pode clicar em Generate a Report (Gerar Relatório) para salvar os resultados como um relatório HTML ou qualquer outro formato preferido.



COMO REALIZAR UM SCAN DE CÓDIGO VIA LINHA DE COMANDOS

1. Siga até o diretório onde o Syhunt está instalado usando o prompt de comandos.
2. Use a seguinte linha de comando:

```
scancode [alvo] -hm:[metodo]]
```

```
# Exemplos:
scancode git://sub.domain.com/repo.git
scancode https://github.com/user/repo.git -rb:master
scancode /source/www/
```

Repositórios TFS e caminhos locais no Windows:

```
// Caminho local
scancode c:\source\www\
scancode c:\source\www\file.php
scancode c:\mobile\myapp.apk
scancode "c:\source code\www\"

// Repositórios TFS
scancode https://dev.azure.com/user/project
scancode https://myserver/tfs/project
scancode collection:https://dev.azure.com/user$/project
```

Os relatórios da ferramenta scancode são gerados e salvos de forma automática a menos que o parâmetro -nr tenha sido fornecido. Você também pode abrir a sessão após o término da varredura através da interface gráfica do Syhunt e usando a opção ≡ Menu -> Past Sessions (Sessões Anteriores).

Os seguintes parâmetros podem ser fornecidos ao chamar a ferramenta scancode, sendo todos eles **opcionais**:

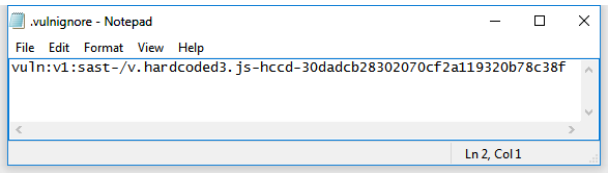
Parâmetro	Descrição	Valor Padrão
sn:[nome]	Um nome de sessão que precisa ser único. Se omitido, um ID único será gerado e atribuido à varredura	ID auto-gerado
hm:[nome]	o método a ser usado durante a varredura. Se omitido, o método padrão será usado	appscan
rb:[branch]	Define o branch do repositório	
tk:[nomedotracker]	Envia resultados para um rastreador após a varredura. Pode ser combinado com o parâmetro -pfcond	
tk2:[nomedotracker]	Mesmo que o indicado acima	

tk3: [nomedotracker]	Mesmo que o indicado acima	
nr	Desliga a geração de um arquivo de relatório ao término de uma varredura	
or	Abre um relatório após a varredura	
rout: [nomedoarquivo]	Define o nome de saída para o relatório e seu formato	Report_[session name].html
rtpl:[nome]	Define o modelo de relatório	Standard
xout: [nomedoarquivo]	Define o nome de saída do export e seu formato	Export_[session name].xml
xout2: [nomedoarquivo]	Define um segundo nome de saída de export e seu formato	Export_[session name].xml
pfcond: [condição]	Define uma condição de aprovação/reprovação a ser relatado	
nv	Desativa o modo verbose. Erro e informações básicas ainda são exibidas	
inc:[modo]	Define o modo de varredura incremental	targetpref
inctag:[nome]	Opcionalmente guarda os dados incrementais associados à uma tag	
refurl:[url]	Define um URL associado com o código-fonte alvo para propósito de referência	
noifa	Desliga a análise de filtragem de entrada durante a varredura	
tml:[tempo]	Define o tempo máximo de uma varredura (ex: 1d, 3h, 2h30m, 50m)	Sem limite
about	Exibe informações sobre a versão atual do Syhunt	
help (ou /?)	Mostra a lista de parâmetros disponíveis	

CARACTERÍSTICAS AVANÇADAS

EVITANDO QUE UMA VULNERABILIDADE DE CÓDIGO SEJA REPORTADA

Você pode impedir que vulnerabilidades específicas sejam reportadas por meio de Ignore IDs ou regras: basta criar um arquivo **.vulnignore** no diretório raiz do repositório de código ou diretório a ser verificado. Cada linha desse arquivo pode conter um Ignore ID ou regra diferente.



Ignore IDs são mostrados em relatórios no final de cada entrada de vulnerabilidade e são a maneira recomendada e mais fácil de ignorar vulnerabilidades no Syhunt. Alternativamente, você pode criar e adicionar Regras de Ignorar que podem se aplicar a cenários mais amplos.

DIFERENÇAS ENTRE OS MÉTODOS DE VARREDURA

Método	Nome na CLI	Tipo	F. Bruta	Injeção	DoS	Demorado
Application Scan (Padrão)	appscan	▤	Y	Y	Y	N
Structure Brute Force	structbf	■	Y (Profundo)	N	N	Y (Very)
Old & Backup Files	fileold	■	Y	N	N	Y
Fault Injection	faultinj	▤	N	Y	Y	N
Top 10 (OWASP)	top10	▤	N	P (TOP10)	Y	N
Top 25 (CWE)	top25cwe	▤	N	P (TOP25)	Y	N
Top 5 (OWASP PHP)	top5php	▤	N	P (TOP5)	N	N
Cross-Site Scripting	xss	▤	N	P (XSS)	N	N
SQL Injection	sqlinj	▤	N	P (SQL)	N	N
File Inclusion	fileinc	▤	N	P (FI)	N	N
Unvalidated Redirects	unvredir	▤	N	P (UR)	N	N
Malware Content	malscan	▤	P (Malware)	P (Malware)	N	N

Passive	passive		N	N	N	N
Spider Only	spider		N	N	N	N
Complete Scan	complete		Y	Y	Y	Y (Very)
Complete Scan, No DoS	compnodos		Y	Y	N	Y (Muito)
Complete Scan, Paranoid	comppnoid		Y (Profundo)	Y	Y	Y (Muito)

Letras: Sim/Não/Parcial (**Y/N/P**)

TIPO DE TESTE

- - Híbrido (Caixa Cinza), Dinâmico e Código
- - Apenas Dinâmico (Caixa Preta)
- - Apenas Código (Caixa Branca)

DEMORADO

Um Sim significa que verificações adicionais e mutações de ataque serão realizadas e que o número de verificações será influenciado pelo número de diretórios encontrados durante o estágio de mapeamento do site.

DESCRIÇÃO

O método Application Scan é o método padrão de scan no Syhunt. Se você desejar utilizar um método diferente de varredura, você poderá selecionar uma das seguintes as opções:

APPLICATION SCAN (SCAN DE APLICAÇÃO)

Identifica falhas em aplicações web que você tenha desenvolvido, no servidor web e em componentes de terceiros. Este método mapeia o web site e realiza ataques contra a estrutura do site e suas aplicações web. Isto inclui procurar por vulnerabilidades de injeção de falhas como XSS, Injeção de SQL, Inclusão de Arquivos, e mais.

STRUCTURE BRUTE FORCE (FORÇA BRUTA DE ESTRUTURA)

Uma força bruta de estrutura verificará por:

- Scripts Comuns Vulneráveis

- Arquivos Comuns
- Vazamento de Banco de Dados
- Backdoors baseadas na Web

O número de verificações será influenciado pelo número de diretórios encontrado durante o estágio de mapeamento do site.

OLD & BACKUP FILES (ARQUIVOS ANTIGOS E DE BACKUPS)

Executa verificações de extensão ao redor da estrutura mapeada de um website.

OWASP TOP 10

Verifica especificamente pelas vulnerabilidades do OWASP Top 10 2017:

1. A1 2017: Injection
2. A2 2017: Broken Authentication
3. A3 2017: Sensitive Data Exposure
4. A4 2017: XML External Entities (XXE)
5. A5 2017: Broken Access Control
6. A6 2017: Security Misconfiguration
7. A7 2017: Cross-Site Scripting (XSS)
8. A8 2017: Insecure Deserialization
9. A9 2017: Using Components with Known Vulnerabilities
10. A10 2017: Insufficient Logging & Monitoring

CWE TOP 25

Verifica especificamente pela lista CWE de Erros Mais Perigosos de Software de 2019.

Confira a lista completa em: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

OWASP PHP TOP 5 (CINCO MAIS DO OWASP)

Verifica especificamente pela Lista das Cinco Principais Vulnerabilidades do PHP, do OWASP:

1. Execução Remota de Comandos
2. Cross-Site Scripting (XSS), incluindo DOM XSS
3. Injeção de SQL
4. Ataques ao Sistema de Arquivos, incluindo Inclusão de Arquivos.

FAULT INJECTION (INJEÇÃO DE FALHAS)

Verifica especificamente por vulnerabilidades de injeção de falhas. Caso este método de varredura seja selecionado, todas as outras verificações que não necessitam de injeção são desligadas e o Syhunt então verificará especificamente por falhas como injeção de SQL, XSS, inclusão de arquivos e outras falhas similares.

CROSS-SITE SCRIPTING (XSS)

Verifica especificamente por vulnerabilidades do tipo XSS, incluindo DOM XSS.

SQL INJECTION (INJEÇÃO DE SQL)

Verifica especificamente por vulnerabilidades de injeção de SQL & NoSQL.

FILE INCLUSION

Verifica especificamente por vulnerabilidades de Inclusão de Arquivos e Directory Traversal.

UNVALIDATED REDIRECTS

Verifica especificamente por vulnerabilidades de Redirecionamento Não-Validado.

MALWARE SCAN

Verifica especificamente por malware, como:

- Web Backdoors
- Conteúdo Malicioso
- Parâmetros de Debug escondidos na aplicação

PASSIVE SCAN

Mapeia a estrutura do web site e reporta vulnerabilidades descobertas sem lançar quaisquer tipos de ataques, como:

1. Vulnerabilidades JavaScript no lado do cliente
2. Diversas fraquezas de formulário
3. Divulgação de tecnologias usadas
4. Cabeçalhos HTTP inseguros
5. Software de Servidor Desatualizado e Vulnerável
6. Scripts Referenciados Desatualizados e Vulneráveis
7. Comentários HTML suspeitos
8. Divulgação de Código Fonte
9. Conteúdo Malicioso sendo servido

SPIDER ONLY

Apenas mapeia a estrutura do website, sem testar por ou reportar qualquer tipo de vulnerabilidade ou fraqueza.

COMPLETE SCAN (SCAN COMPLETO)

Verifica por todos os tipos de vulnerabilidade em aplicações web usando todos os tipos de mutação e métodos de pen-tester, incluindo ataques de Manipulação de Cabeçalho. Um scan completo pode algumas vezes ser bastante demorado quando executado contra um servidor web que possui uma grande quantidade de pastas e pontos de entrada.

COMPLETE SCAN - NO DOS (SCAN COMPLETO - SEM DOS)

O mesmo de antes, mas com os testes de negação de serviço (denial-of-service) desligados.

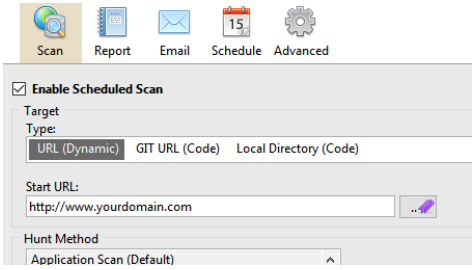
COMPLETE SCAN - PARANOID (SCAN COMPLETO - PARANÓICO)

Verifica por todos os tipos de vulnerabilidades em aplicações web usando força bruta profunda na estrutura do site, todos os tipos de mutações e métodos de pen-tester, incluindo ataques de Manipulação de Cabeçalho. Este método pode ser bastante demorado, especialmente se executado contra grandes sites. Este método tambem realiza uma verificação tripla na força bruta da estrutura, que se aplica a servidores sensíveis a letras maiúsculas e minúsculas - o Syhunt tentará todas as possibilidades de nome de arquivo (tudo em maiúsculas, tudo em minúsculas, etc).

AGENDANDO VARREDURAS

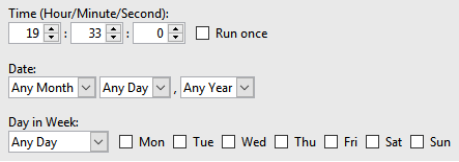
Adicionar e configurar um agendamento é uma tarefa fácil:

1. Clique no ícone Scheduled Scans (Agendamentos) na barra de tarefas inicial. A tela de Scheduled Scans irá abrir.
2. Clique no ícone Add Scheduled Scan (Adicionar Agendamento) na barra da tela Scheduled Scans.
3. Preencha um nome de referência para o novo agendamento (como MeuScan) e pressione **OK**. A janela de preferências irá abrir.
4. Na aba Scan, preencha os detalhes do alvo e selecione o método de varredura e as opções desejadas.



5. Na aba Report (Relatório), configure como desejado as opções de criação de relatório.

6. Na aba Schedule (Cronograma), preencha o plano de evento desejado.

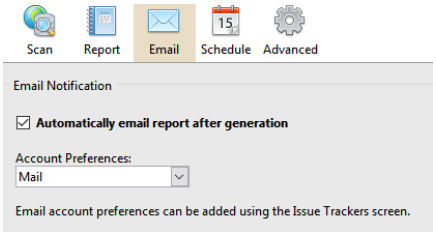


7. Clique no botão **OK** quando estiver tudo pronto.

ENVIANDO RELATÓRIOS POR EMAIL

Em primeiro lugar, você precisa adicionar uma conta de email:

1. Clique no ícone de Issue Trackers (Rastreadores de Problemas) na barra da tela inicial. A tela de Issue Trackers irá abrir.
2. Clique no ícone Add Tracker (Adicionar Rastreador) na barra da tela de rastreadores e escolha a opção do menu Add tracker: Email (Adicionar rastreador: Email).
3. Digite um nome de referência para o novo rastreador (como Mail) e pressione **OK**. A janela de preferências irá abrir.
4. Preencha os endereços de email em Sender/Recipient (Remetente / Destinatário).
5. Preencha o endereço do host e as credenciais em SMTP Authentication (Autenticação de SMTP) e clique no botão **OK**.
6. Clique no ícone Scheduled Scans na barra inicial. A tela Scheduled Scans irá abrir.
7. Clique com o botão direito do mouse em um agendamento e clique na opção Edit Schedule Preferences (Editar Preferências do Agendamento). A janela de preferências irá abrir.
8. Vá até a aba Email e marque a opção **Automatically email report after generation** para ativar o envio de relatório por email.



9. Selecione a conta criada anteriormente.
10. Clique no botão de **OK** quando estiver tudo pronto.

REVENDO RESULTADOS DAS VARREDURAS PROGRAMADAS

A qualquer momento você pode ver os resultados de varreduras atuais ou anteriores e gerar um novo relatório. Apenas abra o Syhunt Hybrid e clique no ícone de **Past Sessions** (Sessões Anteriores) na barra da tela inicial.

TRABALHANDO COM LANÇADORES E AGENDADORES DE TERCEIROS

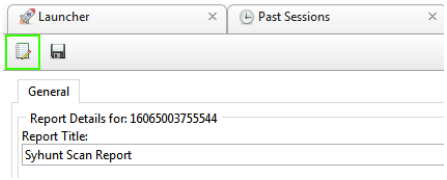
Confira este documento sobre como iniciar o Syhunt a partir de agendadores de terceiros, Jenkins e outras ferramentas

PERSONALIZANDO O RELATÓRIO

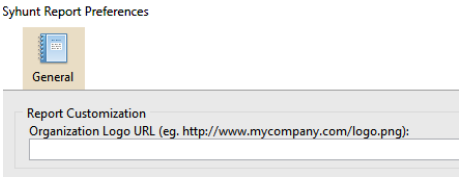
ADICIONANDO UM LOGO AO RELATÓRIO

Antes de salvar um relatório, você pode adicionar um logo que será incluído com os relatórios gerados de agora em diante:

1. Clique no botão Editar Preferências de Relatório (Edit Report Preferences) na barra. O diálogo Preferências de Relatório (Report Preferences) abrirá.



2. Preencha o endereço da imagem contendo o logo



3. Clique OK para guardar as preferências.

Agora ao gerar um relatório, ele irá conter o logo de sua organização em vez do logo da Syhunt.

REQUISITOS DE SISTEMA

O Syhunt (incluindo sua versão Community) deve ser instalado sobre plataformas 64-bit Windows, macOS ou Linux, mas é capaz de analisar aplicações concebidas para qualquer plataforma alvo, incluindo Android, Apple iOS e MacOS, BSD, Linux, Windows, Solaris e Unix, independente da plataforma a partir de qual o software é executado.

1. 4GB de RAM disponível (8GB recomendado)
2. 2GB de espaço livre em disco*
3. Conexão com a Internet (recomendada para quaisquer tipo de varredura e algumas funcionalidades chave)
4. Um dos seguintes sistemas operacionais 64-bit compatíveis:
    1. Windows 7, 8, 10 ou 11, ou Windows Server 2008 a 2019
    2. Ubuntu Server ou Desktop 18 ou posterior
    3. CentOS 7 ou 8 (Minimal ou Everything)

4. Qualquer SO não oficialmente suportado, como as distribuições Linux listadas logo abaixo neste documento, ou o macOS Big Sur ou superior.

5. Java ou Java Headless instalado em SO Linux ou macOS
6. Caso binários nativos não estejam disponíveis para seu tipo ou distribuição de SO específica ainda, o Wine64 Stable (3, 4 ou 5) precisa estar instalado.

Requisitos opcionais:

1. (Opcional) GIT no Linux/macOS ou GIT para Windows instalado, para realizar scans de repositórios GIT
2. (Opcional) Java 8 ou superior, para realizar scans de arquivos APK do Android
3. (Opcional) Python 3.7.0 ou superior, Selenium e navegador Chrome versão 109 ou superior (opcional para recursos estendidos de script)

* Isto não inclui o espaço necessário para salvar os dados de sessões de varreduras, o que varia dependendo do website ou código-fonte alvo de análise e a frequência de varreduras.

DISTRIBUIÇÕES LINUX COMPATÍVEIS

Oficialmente Suportadas:
✔ Ubuntu Server/Desktop 18.10 e posterior
✔ CentOS 7.7 e posterior
Não Oficialmente (Testado com Sucesso):
✔ Kali Linux 2019 e posterior
✔ Parrot OS 4.1, 4.7 e posterior
✔ Debian 9.11 e posterior
✔ Linux Mint 19.2 e posterior
✔ OpenSUSE Leap 15.1 e posterior
✔ Arch Linux 2019 e posterior
✔ Fedora 32
✔ MX Linux 19.1 e posterior
✔ KDE Neon 2020.03 e posterior
✔ Deepin 15.9
✔ Manjaro 19
Não Suportado:
⊘ Elementary OS 5.1 (Testado com Sucesso), 5.0 (Não Suportado)
⊘ CentOS 6.1 (Testado com Sucesso)
⊘ Solus 4.1 (Instável)

CONTATO

FALE CONOSCO